

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

2019 MAY -8 PM 3:50

UNITED STATES OF AMERICA

v.

GILBERT BASALDUA,
JOSEPH PASCUA, and
CRAIG GERMAN

) INDICTMENT NO. **CR 419 069**
)
) 18 U.S.C. § 1832(a)(5)
) Conspiracy to Steal Trade Secrets
)
) 18 U.S.C. § 2314
) Interstate Transportation of Stolen
) Property

THE GRAND JURY CHARGES THAT:

At all times relevant to this Indictment:

1. Company A was a subsidiary of a publicly traded corporation whose business included the design, development, manufacturing, marketing and services of business jet aircraft. Company A sold and shipped jet aircraft, and intended to sell and ship jet aircraft, in the United States and internationally.

2. Company B was a publicly traded corporation whose business included the design, development, manufacturing, marketing and services of aircraft and aerospace technology.

3. Company C was a subsidiary of a publicly traded corporation whose business included the design, development, manufacturing, marketing and services

of jet aircraft. Company C sold and delivered jet aircraft, and intended to sell and deliver jet aircraft, in the United States and internationally.

4. Company D was a business that provided aviation related consulting services, which included designing airplane systems and providing engineering expertise.

Defendants' Employment With Companies A, B and C

5. From on or about October 7, 2016 to November 29, 2018, Defendant **BASALDUA** was employed by Hi-Tek Professionals, Inc. as a contractor, and assigned to work as a numerical control engineer for Company A at one of its facilities in the Southern District of Georgia. In connection with his contract work for Company A, Defendant **BASALDUA** received training and signed agreements regarding the protection of proprietary information.

6. From on or about October 29, 2015 to November 17, 2016, and then again from June 20, 2017 to January 2, 2019, J.M. was employed by third party contractors and assigned to work at Company B at one of its facilities outside the Southern District of Georgia. Most recently, J.M. was assigned to work as a technical lead for a fire and safety group at Company B. In connection with his contract work for Company B and previous employment with other companies, J.M. received training and signed agreements regarding the protection of proprietary information.

7. From on or about 2015 to November 2018, Defendant **PASCUA** was employed by Company B to work as an engineer at Company B at one of its facilities outside the Southern District of Georgia. In connection with his employment with Company B, Defendant **PASCUA** received training and signed agreements regarding the protection of proprietary information.

8. From on or about July 28, 2014 to November 3, 2017, Defendant **GERMAN** was employed by Company C and assigned to work as a cost analyst at one of its facilities outside the Southern District of Georgia. In connection with his employment with Company C, Defendant **GERMAN** received training and signed agreements regarding the protection of proprietary information.

Defendants' Relationships With Company D

9. In approximately 2016, Defendant **PASCUA** agreed to work with Company D to develop an aircraft wing anti-ice product (hereinafter "the product" or "Company D's product"). Defendant **PASCUA** was a principal member of Company D's System Development Team and served as its Vice President of Engineering and Research & Development.

10. On or about December 15, 2017, Defendant **PASCUA** filed a patent on behalf of Company D for the product. Defendant **PASCUA** agreed with the owner and CEO of Company D that the two would share in any profits from sales of the

product (hereinafter “Company D’s profits”).

11. In approximately 2017, Defendant **PASCUA** invited Defendant **BASALDUA** to work with Company D to develop the structural design of the product. Defendant **BASALDUA** agreed to do so in exchange for a share of Company D’s profits, and became Company D’s Vice President of Manufacturing and Product Design.

12. Defendant **BASALDUA** invested approximately \$100,000 into Company D to further its efforts to develop the product. At no time did Defendant **BASALDUA** notify Company A of his relationship with Company D.

13. Sometime in late 2017, Defendants **PASCUA** and **BASALDUA** recruited J.M. to work with Company D as its test configuration engineer. As such, J.M. would develop an icing wind tunnel model for use in testing Company D’s product. J.M. agreed to do so in exchange for a share of Company D’s profits, and became Company D’s Technologies and Wind Tunnel Test Specialist.

14. On a date unknown to the grand jury, but at least as early as June, 2017, Defendant **BASALDUA** recruited Defendant **GERMAN** to conduct cost analyses of Company D’s product. Defendant **GERMAN** agreed to do so in exchange for a share of Company D’s profits, and became Company D’s System Development Team Vice President of Business Development and Supply Chain Management.

Defendants' Marketing and Development Efforts on Behalf of Company D

15. In June and October 2017, J.M. and Defendants **PASCUA**, **BASALDUA** and **GERMAN** presented Company D's product to numerous domestic and international aircraft companies in an effort to get one or more companies to invest in or purchase the product. Each company's response was the same: they were interested in Company D's product, but would not purchase it until it was certified for flight in icing conditions by the Federal Aviation Administration (FAA). Company D's product was not so certified.

16. Aircraft which were "certificated for flight in icing conditions" by the FAA went through an extensive procedure intended to ensure that they could safely operate throughout icing conditions encompassed by the icing envelopes specified by the FAA. The icing certification process included extensive analysis, tunnel testing, dry-air testing, testing behind an icing tanker, and flight in natural icing conditions. The objective was to verify that the aircraft had functioning ice protection and to ensure that the aircraft would have acceptable performance and handling qualities in all the environmental conditions covered by the icing envelopes for which the aircraft had been tested.

17. To obtain FAA certification for the product, J.M. and Defendants **BASALDUA**, **PASCUA** and **GERMAN** needed to develop an icing wind tunnel testing plan and submit the product to the rigorous process described above.

18. To shortcut the process of developing an original icing wind tunnel test plan, J.M. and Defendants **BASALDUA**, **PASCUA** and **GERMAN** agreed to steal proprietary aircraft wing schematics and anti-ice testing documents from other companies, to include Company A and Company C, and to use those documents without authority to develop an icing wind tunnel test plan for the product.

19. By utilizing proprietary aircraft wing schematics and anti-ice documents belonging to other aircraft companies, J.M. and Defendants **BASALDUA**, **PASCUA** and **GERMAN** understood that they could get the product to market faster and with far less expense to Company D.

The Stolen Proprietary Information

20. In particular, the proprietary information the Defendants stole and planned to steal from Company A and Company C contained the following types of valuable and closely-guarded information regarding Company A and Company C aircraft:

- a. aircraft wing schematics, dimensions and detailed measurements;
- b. ice protection system designs, including bleed supply temperatures, mass flows and pressures;

- c. specific detail designs affecting the efficacy of aircraft ice protection and engine thrust;
- d. details regarding how to build an aircraft wing model for testing;
- e. certification testing conditions such as flight profiles, icing severity, system critical conditions, and angles of attack measurements;
- f. control temperatures relating to wing anti-icing and aircraft performance;
- g. step-by-step instructions for creating a certifiable anti-ice protection system throughout the entire icing envelope, to include descent and landing cases;
- h. individual finish and process codes unique to Company A;
- i. a list of materials unique to Company C specifying the parts required for the anti-ice protection system and the prices negotiated for such parts; and
- j. detailed test data, system performance and certification results from lab testing, icing tunnel tests, and dry air testing;

which information is hereinafter referred to as, “anti-ice and wing model information.”

21. The anti-ice and wing model information described above was considered trade secret information by Company A and Company C.

22. Company A protected its anti-ice and wing model information as confidential and proprietary. Company A used a number of reasonable measures to protect its sensitive and proprietary information, including the following:

- a. Company A staffed guards in its main lobby during business hours and deployed a mobile patrol unit to conduct routine patrols 24-hours per day, 7 days per week.
- b. Company A granted physical access to its facilities to only those persons with a valid badge. Company A required all employees, contractors and visitors to have a badge and wear it visibly at all times. Badges could be used to access only those areas that an employee or contractor had a predetermined need to access.
- c. To sponsor a visitor and obtain a visitor badge, a Company A employee had to submit a visitor request including the visitor's name, company affiliation, purpose for visit and citizenship status. Citizenship status information was required because certain areas of Company A are off limits to non-U.S. nationals.
- d. Company A maintained visitor logs in its badging system, and required that visitors be escorted by Company A personnel at all times while in the facility.
- e. Company A implemented data security policies by requiring all new employees and contractors to sign declarations that they have read, reviewed, and agree to abide by Company A's Business Conduct and Ethics Policy, as well as its Use of Computing Systems, Equipment and Support policy. These policies prohibited the unauthorized use or dissemination of sensitive and proprietary information, as well as the use of storage devices and laptops on its computer systems and networks without authorization. Company A confidentiality obligations continue even after an employee or contractor leaves Company A.
- f. Company A employees with access to information about Company A's future programs and activities which had not yet been announced company-wide were required to sign an additional Need To Know document in which they agreed to maintain the confidentiality of that information, even from other Company A employees.
- g. Company A required suppliers, vendors and service providers to execute proprietary information/non-disclosure agreements before they were

allowed to receive any Company A confidential and proprietary information or access Company A facilities.

- h. Company A limited access to its sensitive and proprietary information to those who needed the information to perform their employment duties on Company A's secure electronic database. To obtain access to this database, employees were required to: (1) possess a valid employee badge to enter Company A's main buildings; (2) swipe the badge to access limited-access areas; (3) scan the badge into an employee computer terminal; (4) login with a unique username and password to the Company A network; (5) open a database to which a limited number of employees had access; and (6) login to the database with a unique employee number and password.
- i. Company A tracked searches within its database, such that a system administrator could see what a unique user has searched for and accessed, as well as when the activity occurred.
- j. Company A labeled the front of its reports with a notice indicating that the information was proprietary and that the information could not be disclosed to others without the written authorization of Company A.
- k. Company A prohibited remote access to its database without an approved Company A laptop or cellphone and a VPN token to ensure an encrypted connection.

23. Company C also protected its anti-ice and wing model information as confidential and proprietary. Company C used a number of reasonable measures to protect its trade secrets and its confidential proprietary information, including the following:

- l. Company C implemented data security policies by requiring all new employees and contractors to sign declarations that they have read, reviewed, and agree to abide by Company C's Nondisclosure and Intellectual Property Agreement, and Confidentiality Agreement, and attend training to ensure understanding of these policies. These policies

prohibited the unauthorized use or dissemination of sensitive and proprietary information. Company C confidentiality obligations continue even after an employee or contractor leaves Company C.

- m. Company C employees were required to review the Associate Handbook and sign an acknowledgment that they have reviewed and understand the obligations relating to the handling of confidential and proprietary information as set forth in the handbook.
- n. Company C employees were required to take a training course in information security awareness and renew certification of the class on an annual basis.
- o. Company C employees were required to review the Business Ethics and Conflict of Interest Policy and sign an acknowledgment that they have reviewed and understand the obligations relating to the disclosure of activities, interests, or relationships that have a potential or apparent conflict with Company C as set forth in the policy.
- p. Company C labeled the front of its reports with a notice indicating that the information was proprietary and that the information could not be disclosed to others without the written authorization of Company C.
- q. Company C required vendors and business partners to enter into confidentiality agreements before they were allowed to receive any Company C confidential and proprietary information or access Company C facilities.
- r. Company C granted physical access to its facilities to only those visitors who submitted background information through Company C's electronic visitor request system and signed declarations that they have read, reviewed, and agree to abide by Company C's visitor acknowledgment form, as further described below. The electronic visitor request system required the input of background information, including but not limited to, the purpose for visit, area(s) to be accessed and foreign person status. Foreign Person status information was required because certain areas of Company C are off limits to non-U.S. nationals. The visitor acknowledgment form required visitors to disclose the make or model of any electronic or recording

devices to be brought onto Company C's facilities; to agree not to use any electronic or recording devices to access, download, record, photograph or document any of Company C's designs, processes, networks or other confidential information; and to agree not to utilize any wireless access cards or wireless access points on Company C's facilities.

- s. Company C granted physical access to its facilities to only those persons with a valid badge. Company C required all employees, contractors and visitors to have a badge and wear it visibly at all times. Badges could be used to access only those areas that an employee or contractor had a predetermined need to access. Visitors who entered Company C's confidential work areas were required to be escorted by a Company C representative.
- t. Company C staffed guards at various gate controlled access points on its facilities and deployed a mobile patrol unit to conduct routine patrols 24-hours per day, 7 days per week.
- u. Company C limited access to its sensitive and proprietary information to those who needed the information to perform their employment duties on Company C's secure electronic database. To obtain access to this database, employees were required to login with a unique username and password to the Company C network.
- v. Company C prohibited remote access to its database without an approved Company C laptop or cellphone and a VPN token to ensure an encrypted connection.
- w. Company C prohibited its employees from accessing personal electronic mail accounts and personal cloud-based storage accounts from Company C's network.

COUNT ONE

Conspiracy

18 U.S.C. § 1832(a)(5)

24. The allegations set forth in paragraphs 1-23 of this Indictment are realleged and incorporated herein.

25. Beginning on a date unknown to the grand jury, but at least by in or about June 2017, and continuing until on or about January 2019, within the Southern District of Georgia, and elsewhere, the defendants,

**GILBERT BASALDUA,
JOSEPH PASCUA, and
CRAIG GERMAN**

and others known and unknown to the grand jury, aided and abetted by each other, with some joining the conspiracy earlier and others joining later, did knowingly and willfully combine, conspire, confederate, agree with each other, and others known and unknown to the grand jury, to commit the following offenses:

- a. With intent to convert a trade secret that is related to a product that is used in and intended for use in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will injure any owner of that trade secret, knowingly steal and without authorization appropriate, take, carry away and conceal, and by fraud, artifice, and deception obtain

such information, in violation of Title 18, United States Code, Section 1832(a)(1);

- b. With intent to convert a trade secret that is related to a product that is used in and intended for use in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will injure any owner of that trade secret, knowingly, and without authorization copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information, in violation of Title 18, United States Code, Section 1832(a)(2); and
- c. With intent to convert a trade secret that is related to a product that is used in and intended for use in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will injure any owner of that trade secret, knowingly receive, buy, and possess such information, knowing the same to have been stolen and appropriated, obtained, and converted without authorization, in violation of Title 18, United States Code, Section 1832(a)(3).

Manner and Means

26. J.M. and Defendants **BASALDUA**, **PASCUA**, and **GERMAN** would and did carry out the conspiracy and its unlawful objects, that is the theft, unauthorized taking, carrying away, concealment, copying, download, upload, replication, transmission, delivery, sending, communicating and conveying, receipt, and possession of anti-ice and wing model information owned and controlled by Company A and Company C through the following manner and means, among others:

- a. It was part of the conspiracy that J.M. and Defendants **BASALDUA**, **PASCUA**, and **GERMAN** planned to take, without authority, proprietary documents and engineering drawings from Company A and Company C, which documents contained information that was considered by Company A and Company C to be trade secrets.
- b. It was further part of the conspiracy that J.M. and Defendants **BASALDUA**, **PASCUA**, and **GERMAN** planned to utilize Company A's and Company C's proprietary information, without authority, to create a test plan and test model for conducting icing wind tunnel testing to obtain Federal Aviation Administration (FAA) certification for defendants' aircraft wing anti-ice product.
- c. It was further part of the conspiracy that Defendant **GERMAN** would

send proprietary aircraft wing anti-ice documents and aircraft schematics belonging to Company C to J.M. and Defendants **BASALDUA** and **PASCUA** for use in developing a test plan for Company D's product.

- d. It was further part of the conspiracy that J.M. would provide search terms to Defendant **BASALDUA** to assist Defendant **BASALDUA** in searching Company A systems for its proprietary documents and engineering drawings related to anti-ice test plans and test models.
- e. It was further part of the conspiracy that Defendant **BASALDUA** would search internal Company A networks for anti-ice documents, engineering schematics and aircraft wing drawings.
- f. It was further part of the conspiracy that Defendant **BASALDUA** would download and print Company A's anti-ice documents, engineering schematics and aircraft wing drawings.
- g. It was further part of the conspiracy that Defendant **BASALDUA** would change the file names of Company A's electronic files to conceal their true nature.
- h. It was further part of the conspiracy that Defendant **BASALDUA** would email stolen Company A documents from his Company A email account

to his personal Yahoo email account.

- i. It was further part of the conspiracy that Defendant **BASALDUA** would create scanned electronic copies of stolen Company A documents using commercial copy equipment.
- j. It was further part of the conspiracy that Defendant **BASALDUA** would store electronic copies of stolen Company A documents on his personal electronic storage devices.
- k. It was further part of the conspiracy that Defendant **BASALDUA** would store hard copies of stolen Company A and other aircraft companies' proprietary documents in his residence.
- l. It was further part of the conspiracy that defendant **BASALDUA** would mail or electronically send stolen Company A proprietary material to the other Defendants.
- m. It was further part of the conspiracy that Defendants would share a cloud-based storage account to store and share proprietary information related to development of the aircraft anti-ice technology, to include proprietary information stolen from Company A.
- n. It was further part of the conspiracy that Defendant **PASCUA** would utilize Company A's stolen proprietary engineering schematics,

measurements, dimensions and drawings to design and attempt to design a test article for the Defendants and Company D.

- o. It was further part of the conspiracy that J.M. would utilize Company A's stolen proprietary information to create and attempt to create an icing wind tunnel test plan, with the intent to use the icing wind tunnel test plan to obtain FAA certification for Company D's product.
- p. It was further part of the conspiracy that Defendant **BASALDUA** and others would reserve time at icing wind tunnel testing facilities with the intent to test Company D's product, which tests the Defendants knew would utilize Company A's proprietary information.

27. In furtherance of the conspiracy and to achieve the objects and purposes thereof, J.M. and Defendants **BASALDUA**, **PASCUA**, and **GERMAN** committed and caused to be committed the following overt acts, among others, in the Southern District of Georgia and elsewhere:

- a. On or about June 29, 2017, Defendant **BASALDUA** informed J.M., via text message, that Defendant **GERMAN** might have access to the original test plan to be used as a template for Company D's anti-ice wind tunnel test plan. Defendant **BASALDUA** added, "Please keep that last message confidential."

- b. On or about June 29, 2017, J.M. replied to Defendant **BASALDUA**,
“That is key.”
- c. On or about July 17, 2017, Defendant **GERMAN** downloaded from
Company C’s internal system four proprietary anti-ice documents and
copied them onto a storage device.
- d. On or about October 26, 2017, Defendant **GERMAN** sent two emails
from his Company C email account to his personal email account, which
contained a total of two proprietary anti-ice documents belonging to
Company C.
- e. On or about October 31, 2017, Defendant **GERMAN** presented Company
D’s product to Company A in an effort to recruit Company A as a buyer
and/or investor for the product.
- f. On or about November 19, 2017, Defendant **GERMAN** sent three emails
to Defendant **BASALDUA**, which contained proprietary anti-ice
documents belonging to Company C.
- g. On or about November 19, 2017, Defendant **BASALDUA** forwarded
Defendant **GERMAN**’s emails, containing Company C’s proprietary
anti-ice document, to J.M. and Defendant **PASCUA**.
- h. On or about February 28, 2018, Defendant **GERMAN** sent an email to

J.M., which email contained a different proprietary anti-ice document than the one Defendant **GERMAN** sent on November 19, 2017. In the body of the email, Defendant **GERMAN** wrote, “FYI in case you hadn’t seen this from previous data exchanges from me...”

- i. On or about February 28, 2018, Defendant **GERMAN** sent an email to J.M., which email contained a proprietary Manufacturing Bill of Materials for a Company C aircraft.
- j. On or about March 21, 2018, J.M. instructed **BASALDUA** via text message to search Company A’s internal systems for the “Anti Ice certification plan” of a particular Company A model aircraft.
- k. On or about March 23, 2018, Defendant **BASALDUA** utilized terms relating to anti-ice to search internal Company A systems.
- l. On or about March 23, 2018, Defendant **BASALDUA** used Company A internal systems to view and attempt to view a Company A anti-ice document.
- m. On or about March 27, 2018, Defendant **BASALDUA** utilized terms relating to anti-ice to search internal Company A systems.
- n. On or about March 27, 2018, Defendant **BASALDUA** used Company A internal systems to view and attempt to view approximately 13 Company

A anti-ice documents.

- o. On or about March 27, 2018, Defendant **BASALDUA** viewed and downloaded, from Company A's internal system, a Company A proprietary anti-ice document ending in 1875.
- p. On or about March 27, 2018, Defendant **BASALDUA** sent a text message to J.M. stating, "I believe I found the test plan."
- q. On or about March 27, 2018, Defendant **BASALDUA** emailed J.M. and Defendants **GERMAN**, and **PASCUA** a Company A proprietary anti-ice document ending in 1875 with a message stating, "Here you go guard this, my job depends on it."
- r. On or about April 2, 2018, Defendant **BASALDUA** sent a text message to Defendants **GERMAN** and **PASCUA** with a message stating, "Were you able to get the CATIA Files Craig sent open."
- s. On or about April 2, 2018, Defendant **PASCUA** sent a text message to Defendant **BASALDUA** stating, "I have the email, I'll open the [Company A model] files today when I get home."
- t. On or about April 6, 2018, J.M. sent Defendant **BASALDUA** an email with an attachment titled, "Anti-Ice_Plan.docx," which was a preliminary draft of Company D's icing tunnel test plan. In the email,

J.M. stated, "I still need a lot of information."

- u. On or about April 12, 2018, J.M. asked Defendant **BASALDUA** via text message to search Company A internal systems for information pertaining to "cabin pressurization system," "outflow valve," or "outflow valve system."
- v. On or about April 13, 2018, Defendant **BASALDUA** sent J.M. the title of a Company A document via text message, but stated, "I am not allowed access."
- w. On or about April 13, 2018, Defendant **BASALDUA** informed J.M. via text message, "I should have what you need. 6 docs about 300 pages. Should be somewhere in there."
- x. On or about April 13, 2018, J.M. replied via text message, "Cool Please mail it here," and provided his mailing address.
- y. On or about June 21, 2018, J.M. sent a text message to Defendant **BASALDUA** reading, "Gilbert I need a couple of documents. I'll send the numbers in a few."
- z. On or about June 21, 2018, Defendant **BASALDUA** replied, "Ok," after which J.M. sent the names of two Company A proprietary documents ending in 1874 and 1219.

- aa. On or about June 22, 2018, Defendant **BASALDUA** accessed Company A internal systems and viewed a Company A proprietary anti-ice document ending in 1874.
- bb. On or about June 22, 2018, Defendant **BASALDUA** told J.M., via text message, “Got both docs.”
- cc. On about June 24, 2018, Defendant **BASALDUA** visited a commercial copying business in Hilton Head, SC, and created a scanned copy of a Company A proprietary anti-ice document, the document number of which ended in 1874.
- dd. On or about June 24, 2018, Defendant **BASALDUA** emailed Company A’s proprietary anti-ice document ending in 1874 to J.M. as an attachment titled, “Staples Scan.pdf.”
- ee. On or about November 12, 2018, J.M. asked Defendant **BASALDUA** via email to obtain specific Company A proprietary documents ending in 0498 and 1290.
- ff. On or about November 19, 2018, Defendant **BASALDUA** sent a text message to J.M. and Defendant **PASCUA**, notifying them that he had uploaded a Company A proprietary ice tunnel testing document to a cloud storage space for them to view.

gg. On or about November 21, 2018, Defendant **BASALDUA** sent an email from his Company A email account to his personal Yahoo account titled, "Time Card," with an attachment titled, "Wing.ppt." The attachment titled, "Wing.ppt" contained a PowerPoint file with engineering drawings of a Company A aircraft wing.

hh. Between on or about November 13-28, 2018, Defendant **BASALDUA** accessed internal Company A systems to view and attempt to view multiple Company A proprietary anti-ice documents and wing drawings.

ii. On or about November 13, 2018, Defendant **BASALDUA** accessed internal Company A systems to view a Company A proprietary anti-ice document ending in 1290.

jj. Between on or about November 13-27, 2018, Defendant **BASALDUA** downloaded the Company A proprietary anti-ice document ending in 1290 and changed the file name to "Time Card."

kk. On or about November 27, 2018, Defendant **BASALDUA** emailed the Company A proprietary anti-ice document ending in 1290, now titled, "Time Card," from his Company A email account to his personal Yahoo account.

ll. On or about December 10, 2018, J.M. emailed Defendants **PASCUA** and

BASALDUA about scheduling the icing wind tunnel testing of Company D's product in January or February 2019. The email contained a proposed Company D nondisclosure agreement, which agreement defined the term, "proprietary information" and addressed all parties' obligations to protect such information.

All in violation of Title 18, United States Code, Section 1832(a)(5).

COUNT TWO

Interstate Transportation of Stolen Property

18 U.S.C. § 2314

28. The allegations set forth in paragraphs 1-23 of this Indictment are realleged and incorporated herein.

29. On or between October 16, 2016 and November 29, 2018, the exact dates being unknown to the grand jury, in the Southern District of Georgia, the defendant,

GILBERT BASALDUA,

did unlawfully transport, transmit, and transfer in interstate commerce from Chatham County, Georgia, to Beaufort County, South Carolina, the following stolen goods belonging to Company A, each item having a value of \$5,000 or more, knowing the same to have been stolen, converted, and taken by fraud:

- a. Document bearing Company A proprietary markings with title ending in 6862;
- b. Document bearing Company A proprietary markings with title ending in 1874;
- c. Document bearing Company A proprietary markings with title ending in 1875;
- d. Document bearing Company A proprietary markings with title ending in 1290; and
- e. Document bearing Company A proprietary markings with title ending in 14A.

All in violation of Title 18, United States Code, Section 2314.

FORFEITURE ALLEGATIONS

The allegations contained in Counts One and Two of this Indictment are hereby re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 981, 2323, and Title 28, United States Code, Section 2461.

25. Upon conviction of Title 18, United States Code, Section 1832(a)(5), set forth in Count One of this Indictment, the Defendants,

**GILBERT BASALDUA
JOSEPH PASCUA, and
CRAIG GERMAN**

shall forfeit to the United States pursuant to Title 18, United States Code, Section 2323, any article, the making or trafficking of which is prohibited, and any property used, or intended to be used in any manner or part to commit or facilitate the commission of prohibited activity, as well as any property constituting or derived for any proceeds obtained directly or indirectly as a result of the commission of the prohibited activity.

26. Upon conviction of the Title 18, United State Code, Section 2314, set forth in Counts Two and Three, the Defendant **GILBERT BASALDUA**, shall forfeit to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) and 28, United States Code, Section 2461, any property, real or personal, which

constitute or is derived from proceeds traceable, or involved in the offense and any property traceable to the offense.

26. If any of the property described above, as a result of any act or omission of the Defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c).

shall forfeit to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C), 982(a)(1), 18 U.S.C. § 1834(a)(1) and 28 U.S.C. § 2461, any property, real or personal, constituting or derived from, the proceeds they obtained directly or indirectly as a result of the offenses in Count(s) 1 and 2 of the Indictment, and any property traceable to such property including, but not limited to the following:

- a. One iBuy Power Desktop computer with purple thumb drive (serial number 5946-AC69-6362-9B90);
- b. One Kingston purple thumb drive;
- c. One Simpletech External Hard Drive;
- d. One Microsoft Surface Pro laptop (serial number 012985365353);
- e. One Microsoft tablet device (identification number E3E19E3B-C966-45E3-9BC4-1E777A7B0E99);
- f. One Apple iPhone (IMEI number 352065062748220); and
- g. One Samsung Galaxy Note 8 SM-N95OU cell phone (serial number R58J95AW7XW).
- h. A money judgment for a sum of money equal to all of the proceeds obtained as a result of the offense listed in this Indictment.

XX. If, as a result of any act or omission of the defendants, any property subject to forfeiture:

- A. Cannot be located upon the exercise of due diligence;
- B. has been transferred or sold to, or deposited with, a third person;
- C. has been placed beyond the jurisdiction of the Court;

D. has been substantially diminished in value; or

E. has been co-mingled with other property which cannot be subdivided without difficulty; the United States intends, pursuant Title 21 United States Code, Section 853(p), as incorporated by Title 18 United States Code, Section 982(b), to seek forfeiture of any other property of said defendant up to the value of the forfeitable property.

All in violation of 18 U.S.C. §§ 981(a)(1)(C), 982(a)(1), 982(b)(2), 1834(a)(1) and 28 U.S.C. § 2461.

FORFEITURE (*Instrumentalities*)

XX. Upon conviction of the offenses alleged in Counts 1 and 2, the defendants,

**GILBERT BASALDUA
JOSEPH PASCUA, and
CRAIG GERMAN**



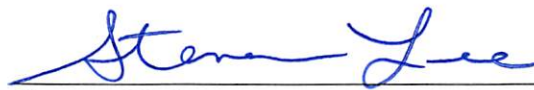
shall forfeit to the United States any property used, or intended to be used, in any property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of said violation, including but not limited to the following property:

- i. One iBuy Power Desktop computer with purple thumb drive (serial number 5946-AC69-6362-9B90);
- j. One Kingston purple thumb drive;
- k. One Simpletech External Hard Drive;
- l. One Microsoft Surface Pro laptop (serial number 012985365353);

- m. One Microsoft tablet device (identification number E3E19E3B-C966-45E3-9BC4-1E777A7B0E99);
- n. One Apple iPhone (IMEI number 352065062748220); and
- o. One Samsung Galaxy Note 8 SM-N95OU cell phone (serial number R58J95AW7XW).

All in violation of Title 18, United States Code, Section 1834.

A True Bill.


Bobby L. Christine
United States Attorney
Brian T. Rafferty
Assistant United States Attorney
Chief, Criminal Division
Jennifer G. Solari
Assistant United States Attorney
Deputy Chief, Criminal Division
*Lead Counsel
Steven H. Lee
Assistant United States Attorney
*Co-lead Counsel